PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-264178
(43)Date of publication of application : 13.10.1995

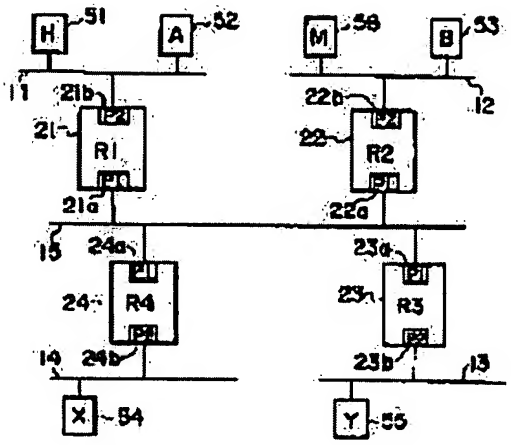
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
G06F 13/00
G06F 15/00
H04L 12/40

(21)Application number : 06-052212
(22)Date of filing : 23.03.1994

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : ITAGAKI KANJI

(54) SECURITY SYSTEM

(57)Abstract:
PURPOSE: To obtain the security system in which illegal access is inhibited and an address accessed illegally is located.
CONSTITUTION: The system is provided with repeaters 21-24 informing alarm information when illegal access takes place to terminal equipments 51-55 on LANs 11-14 connecting to a concerned repeater from any of the terminal equipments 51-55 and a management equipment 56 displaying the content when alarm information is received. The management equipment 56 retrieves to which port of each of the repeaters 21-24 the terminal equipment making illegal access is connected based on the alarm information and the access history information having each of the repeaters 21-24 to locate to which LAN the terminal equipment is connected.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－264178

(43)公開日　平成７年(1995)10月13日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00				
9/10				
9/12				
			Ｈ０４Ｌ　9/00　Ｚ	
			11/00　３２０	

審査請求　未請求　請求項の数８　ＯＬ　（全９頁）　最終頁に続く

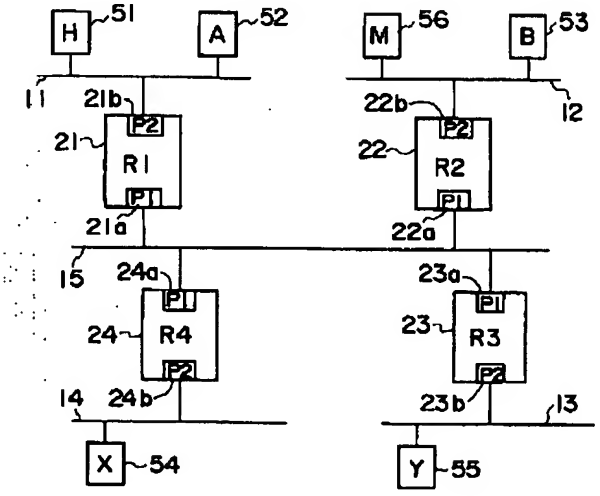
(21)出願番号　特願平6－52212

(22)出願日　平成６年(1994)３月23日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　板垣　寛二
神奈川県鎌倉市上町屋325番地　三菱電機株式会社コンピュータ製作所内
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　セキュリティ方式

(57)【要約】
【目的】　不正アクセスを禁止するのみならず不正アクセスをした箇所を特定することのできるセキュリティ方式を提供する。
【構成】　いずれかの端末装置５１～５５から自中継装置に接続されたＬＡＮ１１～１４上の端末装置５１～５５に対して不正アクセスがあった場合、アラーム情報を通知する中継装置２１～２４と、アラーム情報を受信するとその内容を表示する管理装置５６と、を有するネットワークシステムにおいて、管理装置５６は、アラーム情報と各中継装置２１～２４が有するアクセス履歴情報とから不正アクセスをした端末装置が各中継装置２１～２４のどちら側のポートに接続されているかを絞り込んでいくことで、どのＬＡＮ上に接続されているかを特定する。



1

【特許請求の範囲】

【請求項１】　固有のアドレスが割り付けられた端末装置を接続する伝送媒体と、

前記伝送媒体を介して前記端末装置管の通信を中継する中継装置と、

いずれかの前記伝送媒体に接続されネットワークシステムを管理する管理装置と、

を有し、許可された各端末装置間の通信を行わせるセキュリティ方式において、

前記中継装置は、自中継装置に接続されている前記伝送媒体上の前記端末装置に対する不正アクセスまたは障害を検出すると、アラーム情報を前記管理装置に通知することを特徴とするセキュリティ方式。

【請求項２】　請求項１記載のセキュリティ方式において、

前記中継装置は、前記アラーム情報を通知する条件を登録するアラーム通知条件登録手段を有することを特徴とするセキュリティ方式。

【請求項３】　請求項１記載のセキュリティ方式において、

前記管理装置は、受信したアラーム情報を表示する手段を有することを特徴とするセキュリティ方式。

【請求項４】　請求項１記載のセキュリティ方式において、

前記管理装置は、任意の前記中継装置に対し、自中継装置に接続されている前記伝送媒体を介してのアクセス状況を記録したアクセス履歴情報の送信を要求する手段を有することを特徴とするセキュリティ方式。

【請求項５】　請求項４記載のセキュリティ方式において、

前記管理装置は、前記中継装置から受信した前記アクセス履歴情報と前記アラーム情報とから不正アクセスをした前記端末装置が接続されている前記伝送媒体を特定する手段を有することを特徴とするセキュリティ方式。

【請求項６】　請求項４記載のセキュリティ方式において、

前記管理装置は、前記中継装置から受信した前記アラーム情報から前記端末装置を特定する手段を有することを特徴とするセキュリティ方式。

【請求項７】　請求項１及び請求項３乃至請求項６記載のセキュリティ方式において、

前記各管理装置は、前記端末装置により実現することを特徴とするセキュリティ方式。

【請求項８】　請求項１記載のセキュリティ方式において、

前記中継装置は、設定されている許可／禁止情報に基づき受信したフレームの中継制御の許可／禁止の判断を行い、中継制御を禁止すると判断した場合において設定されているアラーム情報通知条件に基づき不正アクセスまたは障害を検出することを特徴とするセキュリティ方式。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、セキュリティ方式、特に複数のローカルエリアネットワーク（以下、ＬＡＮという）あるいは公衆網等の伝送媒体により構築されるネットワークシステムにおいて、禁止された端末装置に不正にアクセスをしようとした端末装置を突き止めるセキュリティ方式に関する。

【０００２】

【従来の技術】従来からブリッジ、ルータ等の中継装置を介して複数のＬＡＮを接続して構築するネットワークシステムにおいて、異なるＬＡＮに接続された端末装置間の通信可不可等のアクセス制御を行うために各種セキュリティ方式が採用されている。

【０００３】例えば、特開平３－２８０６３９号公報には、各種テーブルを用いて許可されていない端末装置からの不正アクセスを禁止する方式が記載されている。図８は、この特開平３－２８０６３９号公報に開示された従来のローカルエリアネットワークシステムの構成図である。

【０００４】幹線ＬＡＮ１と各支線ＬＡＮ２－１～２－４は、それぞれアドレスＮＡ１～ＮＡ４が割り当てられたノード装置Ｎ２１～Ｎ２４で接続されている。支線ＬＡＮ２－１～２－４のいずれかには固有のアドレスＴＡ１～ＴＡ５が割り当てられた端末装置Ｔが、また支線ＬＡＮ２－１にはアドレスＮＭＡが割り当てられたネットワーク管理局ＮＭＳが、それぞれ接続されている。また、ノード装置Ｎ２１、Ｎ２２はグループ番号Ｇ１のグループ、ノード装置Ｎ２３、Ｎ２４グループ番号Ｇ２のグループとしてグループ化されている。

【０００５】各ノード装置Ｎ２１～Ｎ２４は、自ノード装置に接続された支線ＬＡＮ２－１～２－４に接続された端末装置Ｔのアドレスを登録する支線側フィルタリングテーブルＴＢＳ１～ＴＢＳ４と、自ノード装置に接続されていない、すなわち自ノード装置から見て幹線ＬＡＮ１側に接続された端末装置Ｔのアドレスを登録する幹線側フィルタリングテーブルＴＢＫ１～ＴＢＫ４と、特権端末装置のアドレスを登録する特権端末テーブルＴＴＢ１～ＴＴＢ４と、ネットワーク管理局ＮＭＳのアドレスＮＭＡを登録するＮＭＳアドレステーブルＮＴＢ１～ＮＴＢ４と、をそれぞれ有している。

【０００６】次に、この従来例において、アドレスＴＡ３の端末装置Ｔ（以下、端末装置Ｔ（ＴＡ３）と記す）からアクセスが許可されていない端末装置Ｔ（ＴＡ４）に対してフレームを送信する場合の動作を説明する。なお、通信に使用されるフレームには、宛先アドレス、発信元アドレスが含まれている。

【０００７】ノード装置Ｎ２２は、端末装置Ｔ（ＴＡ

３）からフレームを受信すると、自支線ＬＡＮ２－２に端末装置Ｔ（ＴＡ４）が接続されていないことから明らかなように、支線側フィルタリングテーブルＴＢＳ２に宛先となる端末装置Ｔ（ＴＡ４）のアドレスＴＡ４が登録されていないので、フレームにグループ番号Ｇ１をのせて幹線ＬＡＮ１に転送する。

【０００８】ノード装置Ｎ２３は、幹線ＬＡＮ１から受信した当該フレームには自ノード装置と異なるグループ番号が書き込まれていることを確認した後、以下の手順で処理を行う。

【０００９】まず、当該フレームの宛先アドレスの内容をＮＭＳアドレステーブルＮＴＢ３の中から検索する。発信元となる端末装置Ｔ（ＴＡ３）のアドレスＴＡ３は登録されていないので、次に当該フレームの発信元アドレスの内容を特権端末テーブルＴＴＢ３の中から検索する。端末装置Ｔ（ＴＡ３）のアドレスＴＡ３は登録されていないので、次に当該フレームの発信元アドレスの内容をＮＭＳアドレステーブルＮＴＢ３の中から検索する。端末装置Ｔ（ＴＡ３）のアドレスＴＡ３は登録されていないので、その結果、当該フレームは廃棄される。

【００１０】このようにして、従来例におけるノード装置Ｎ２１～Ｎ２４は、アクセスが許可されていない端末装置Ｔからのフレームを廃棄することで不正アクセスを禁止していた。

【００１１】

【発明が解決しようとする課題】しかしながら、従来においては、上記のようにフレームを廃棄することで不正アクセスを禁止することはできても不正にアクセスしようとした事実を知ることはできない。従って、どの端末装置から不正にアクセスしようとしたということを知ることはできない。

【００１２】本発明は以上のような問題を解決するためになされたものであり、その目的は、不正アクセスを禁止するのみならず不正アクセスをした箇所を特定することのできるセキュリティ方式を提供することにある。

【００１３】

【課題を解決するための手段】以上のような目的を達成するために、請求項１記載の発明は、固有のアドレスが割り付けられた端末装置を接続する伝送媒体と、前記伝送媒体を介して前記端末装置管の通信を中継する中継装置と、いずれかの前記伝送媒体に接続されネットワークシステムを管理する管理装置と、を有し、許可された各端末装置間のみの通信を行わせるセキュリティ方式において、前記中継装置は、自中継装置に接続されている前記伝送媒体上の前記端末装置に対する不正アクセスまたは障害を検出すると、アラーム情報を前記管理装置に通知することを特徴とする。

【００１４】請求項２記載の発明は、請求項１記載のセキュリティ方式において、前記中継装置は、前記アラーム情報を通知する条件を登録するアラーム通知条件登録手段を有することを特徴とする。

【００１５】請求項３記載の発明は、請求項１記載のセキュリティ方式において、前記管理装置は、受信したアラーム情報を表示する手段を有することを特徴とする。

【００１６】請求項４記載の発明は、請求項１記載のセキュリティ方式において、前記管理装置は、任意の前記中継装置に対し、自中継装置に接続されている前記伝送媒体を介してのアクセス状況を記録したアクセス履歴情報の送信を要求する手段を有することを特徴とする。

【００１７】請求項５記載の発明は、請求項４記載のセキュリティ方式において、前記管理装置は、前記中継装置から受信した前記アクセス履歴情報と前記アラーム情報とから不正アクセスをした前記端末装置が接続されている前記伝送媒体を特定する手段を有することを特徴とする。

【００１８】請求項６記載の発明は、請求項４記載のセキュリティ方式において、前記管理装置は、前記中継装置から受信した前記アラーム情報から前記端末装置を特定する手段を有することを特徴とする。

【００１９】請求項７記載の発明は、請求項１及び請求項３乃至請求項６記載のセキュリティ方式において、前記各管理装置は、端末装置により実現することを特徴とする。

【００２０】請求項８記載の発明は、請求項１記載のセキュリティ方式において、前記中継装置は、設定されている許可／禁止情報に基づき受信したフレームの中継制御の許可／禁止の判断を行い、中継制御を禁止すると判断した場合において設定されているアラーム情報通知条件に基づき不正アクセスまたは障害を検出することを特徴とする。

【００２１】

【作用】以上のような構成を有する本発明に係るセキュリティ方式においては、中継装置は不正アクセスを検出すると、アラーム情報を管理装置に通知するので、管理装置は、不正アクセスがあったことを検出することができ、その内容を表示することでネットワーク管理者等に知らせることができる。

【００２２】アラーム通知条件登録手段は、アラーム情報を管理装置に通知する条件を設定登録することができる。

【００２３】管理装置は、任意の中継装置に対しアクセス履歴情報の送信を要求し、その結果得られたアクセス履歴情報とアラーム情報とから不正アクセスをした前記端末装置が接続されている伝送媒体を特定することができる。

【００２４】また、管理装置は、任意の中継装置に対しアクセス履歴情報の送信を要求し、その結果得られたアラーム情報から不正アクセスをした前記端末装置を特定することができる。

【００２５】また、中継装置は、設定されている許可／

禁止情報に基づき受信したフレームの中継制御の許可／禁止の判断を行う。その結果、中継制御を禁止すると判断した場合、設定されているアラーム情報通知条件に基づいて、アラーム通知の必要性があるかどうかを判断する。必要性があると判断することにより不正アクセスまたは障害を検出するとし、アラーム情報を管理装置に通知する。従って、管理装置は、不正アクセスがあったことを検出することができる。

【００２６】

【実施例】以下、図面に基づいて、本発明の好適な実施例を説明する。

【００２７】図１は、本実施例におけるセキュリティ方式が実施されるネットワークシステムの構成図である。

【００２８】伝送媒体であるＬＡＮ１１、１２、１３、１４、１５は、それぞれ中継装置２１、２２、２３、２４で接続されている。各ＬＡＮ１１、１２、１３、１４、１５のいずれかには、それぞれに固有のアドレスが割り当てられた端末装置５１、５２、５３、５４、５５が接続されており、各端末装置５１～５５は、物理的に各ＬＡＮ１１～１５、中継装置２１～２４を介して通信可能である。また、ＬＡＮ１２には、端末装置であってネットワークシステム全体を管理する管理装置５６が接続されている。各中継装置２１～２４は、ＬＡＮ１１～１５を物理的に接続するポートを有している。もちろん、３つ以上のポートを有してもよいが、図に示したように本実施例における各中継装置２１～２４は、それぞれ２本のＬＡＮを接続しているためそれぞれ２つのポート番号Ｐ１、Ｐ２のポート２１ａ、２１ｂ、２２ａ、２２ｂ、２３ａ、２４ｂ、２４ａ、２４ｂを有している。

【００２９】図２は、中継装置２１の構成を示した図である。中継装置２１は、前述したポート２１ａ、２１ｂと、中継装置２１における処理を制御する制御部２１ｃと、中継を許可／禁止する端末装置に関する情報が登録されている中継制御テーブル２１ｄと、を有する。この中継制御テーブル２１ｄに登録する情報としては、特権端末装置のアドレス、管理装置５６のアドレス等がある。更に、本実施例における中継装置２１は、不正アクセスまたは障害があったときなどに管理装置５６にアラーム情報をポートを介して通知するアクセス情報通知部２１ｅと、管理装置５６にアラーム情報を通知すべき条件を登録するアラーム情報通知条件登録部２１ｆと、を有することを特徴とする。これにより、不正アクセス等があったことを管理装置５６に通知することができる。更に、また本実施例における中継装置２１は、自中継装置２１に接続されているＬＡＮ１１、１５を介してのアクセス状況、すなわちどの端末装置からどの端末装置へのアクセス要求があったかのアクセス履歴を記録するアクセス履歴情報記憶部２１ｇを有することを特徴とする。図３は、中継装置２１～２４それぞれが有しているアクセス履歴情報であり、端末装置間通信で使用されるフレームを受信した側のポート番号とフレームの発信元となる端末装置のアドレスとが対応づけられて記録される。これにより、フレームの発信元となる端末装置が中継装置２１～２４のどちら側のＬＡＮに存在するかを知ることができる。他の中継装置２２、２３、２４も同様の構成である。なお、本実施例における端末装置間通信に使用されるフレームには、少なくとも発信元アドレスと宛先アドレスとが含まれている必要がある。

【００３０】図４は、管理装置５６の構成を示した図である。管理装置５６は、ＬＡＮ１２を介して他の装置との間でフレーム等の送受信を行う入出力部５６ａと、本装置における処理を制御する制御部５６ｂと、メモリ５６ｃと、を有する。更に、本実施例における管理装置５６は、中継装置２１～２４から受信したアラーム情報を表示するアラーム情報表示部５６ｄを有することを特徴としており、これにより、いずれかの端末装置への不正アクセスがあったという事実を即座にシステム管理者等に知らせることができる。更に、また本実施例における管理装置５６は、任意の中継装置２１～２４に対して各中継装置２１～２４が記憶しているアクセス履歴情報の送信を要求しうるアクセス履歴情報送信要求部５６ｅを有することを特徴としており、これにより、管理装置５６において、どの端末装置５１～５５が中継装置２１～２４のどちら側に存在しているかを知ることができる。

【００３１】図５は、本実施例における中継装置２１～２４の処理を示したフローチャートであり、以下、これに基づいて本実施例における中継装置２１～２４の動作について説明する。

【００３２】例として端末装置５４から端末装置５１にフレームを送信（アクセス）する場合を説明する。

【００３３】まず、各中継装置２１～２４の中継制御テーブル２１ｄに何も設定されていない場合について説明する。

【００３４】中継装置２４は、端末装置５４からフレームをＬＡＮ１４、ポート２４ｂを介して受信すると、アクセス履歴情報記憶部２１ｇに端末装置５４のアドレス（Ｘ＿ａｄｒ）と受信したポート番号Ｐ２を対応づけて記憶（保存）する（ステップ１０１）。なお、ポート２４ａ、２４ｂに接続されているＬＡＮ１４、１５上の端末装置は、予めアクセス履歴情報記憶部２１ｇに設定しておいてもよい。ここで、中継制御テーブル２１ｄに設定があるかを判断する（ステップ１０２）。この場合、設定がないので、次に、フレーム受信したポート番号は、アクセス履歴情報において端末装置５１のアドレス（Ｈ＿ａｄｒ）は、端末装置５４と同じポート番号であるかを比較参照する（ステップ１０３）。仮に、端末装置５１が端末装置５４と同じポート番号Ｐ２であれば、端末装置５１は同一のＬＡＮ１４上にあると判断され、そのフレームを他のＬＡＮ上に送出する必要はない。従って、当該フレームを廃棄する（ステップ１０８）。ま

た、端末装置５１が端末装置５４と同じポート番号Ｐ２でなければ、そのポートからフレームを送出する（ステップ１０９）。本実施例においては、ポート番号Ｐ１からフレームを送出する。なお、端末装置５１のアドレスがまだ記憶されていなければ、当該フレームを受信したポート以外のポート２４ａから送出する（ステップ１０９）。ポート２４ａから送出されたフレームは、ＬＡＮ１５に接続されている中継装置２１、２２、２３により受信される。フレームを受信すると、各中継装置２１、２２、２３におけるアクセス履歴情報記憶部２１ｇに端末装置５４のアドレス（Ｘ＿ａｄｒ）と受信したポート番号Ｐ１を対応づけて記憶する（ステップ１０１）。ここで、各中継装置２１、２２、２３において、フレーム内の宛先アドレス（この例においてはＨ＿ａｄｒ）を参照し、自アクセス履歴情報記憶部２１ｇに宛先アドレスと受信したポート以外のポート番号（本実施例においてはＰ２のみ）とで対応づけられたアクセス履歴情報があるかを検索する。この例においては、中継装置２１のアクセス履歴情報記憶部２１ｇに記録されているので、中継装置２１のみがポート２１ｂからフレームを送出する。他の中継装置２２、２３は、当該フレームを廃棄する。

【００３５】このようにして、各中継装置２１～２４の中継制御テーブル２１ｄに何も設定されていない場合、端末装置５１は、ＬＡＮ１１を介して端末装置５４から送出されたフレームを受信することができる。

【００３６】次に、中継装置２１の中継制御テーブル２１ｄに端末装置への許可／禁止情報が設定登録されている場合について説明する。本実施例においては、以下の許可／禁止情報（１）及び（２）が設定されているものとする。

【００３７】（１）端末装置５１と端末装置５３との間の双方向のフレームの中継を許可する。

【００３８】（２）ＬＡＮ１３、１４に接続されている端末装置からのフレームの中継を禁止する。

【００３９】また、中継装置２１のアラーム情報条件登録部２１ｆに、ＬＡＮ１３、１４に接続されている端末装置からフレームを受信した場合、アラーム情報を通知するという条件を登録しておく。

【００４０】このように設定された場合であっても、端末装置５１、５２、５３間でのフレーム送受信、すなわちアクセスは可能である。また、端末装置５３、５４、５５間のアクセスも可能である。

【００４１】ここで、上記と同様、端末装置５４から端末装置５１にフレームを送信（アクセス）する場合について説明するが、主要でない上記と同様の動作についての説明は省略する。

【００４２】端末装置５４がフレームを送出すると、中継装置２４は、端末装置５４からフレームをＬＡＮ１４、ポート２４ｂを介して受信し、アクセス履歴情報記憶部２１ｇに端末装置５４のアドレス（Ｘ＿ａｄｒ）と受信したポート番号Ｐ２を対応づけて記憶（保存）する（ステップ１０１）。ここで、中継装置２４の中継制御テーブル２１ｄには何も設定されていないので（ステップ１０２）、上記と同様、ポート番号Ｐ１から当該フレームを送出する（ステップ１０９）。

【００４３】中継装置２１は、中継装置２４からのフレームを受信すると、アクセス履歴情報記憶部２１ｇに端末装置５４のアドレス（Ｘ＿ａｄｒ）と受信したポート番号Ｐ１を対応づけて記憶する（ステップ１０１）。ここで、中継制御テーブル２１ｄに設定があるかを判断する（ステップ１０２）。この場合、設定があるので、次に、中継制御が許可されているかを判断する（ステップ１０４）。前述したとおり、中継装置２１の中継制御テーブル２１ｄには前述したとおり許可／禁止情報（１）、（２）が設定されているので、許可された中継制御は、端末装置５１と端末装置５３との間の双方向のフレームの中継のみである。次に、中継制御が禁止されているかを判断する（ステップ１０５）。前述したとおり、この例のＬＡＮ１４に接続されている端末装置２４からのフレームの中継は禁止されているので、次にアラーム情報通知部２１ｅにおいてアラーム通知の必要性を判断する（ステップ１０６）。前述したように、中継装置２１のアラーム情報条件登録部２１ｆには、ＬＡＮ１４に接続されている端末装置５４からフレームを受信した場合、アラーム情報を通知するという条件が登録されているので、アラーム情報通知部２１ｅは、ポート２１ａからアラーム情報を管理装置５６に通知する（ステップ１０７）。この通知されるアラーム情報には、アラーム情報発送元となる中継装置を特定できるアドレス等の情報、フレームの発信元、宛先となる端末装置のアドレス等が含まれている。中継装置２１は、アラーム情報通知後、当該フレームを廃棄する（ステップ１０８）。

【００４４】以上のようにして、不正アクセスを検出したいずれかの中継装置２１～２４は、管理装置５６にアラーム情報を通知することができる。

【００４５】次に、アラーム情報を受信した後の管理装置５６における動作について説明する。

【００４６】管理装置５６は、入出力部５６ａを介してアラーム情報を受信すると、その内容をメモリ５６ｃに記憶するとともにアラーム情報表示部５６ｄによりＣＲＴ、プリンタ等の出力装置に表示させる。これにより、管理装置５６が管理するネットワークシステムにおいて不正アクセスまたは障害があったことをネットワーク管理者等に知らせることができる。

【００４７】また、本実施例においては、不正アクセスがあったことを知ることができるのみならず、不正アクセスをした端末装置がどの中継装置に接続されたＬＡＮ上にあるかを特定することができることを特徴とする。以下、このＬＡＮを特定する動作について説明する。

【００４８】管理装置５６は、受信したアラーム情報の内容からアラーム情報を発した中継装置を特定することができるので、アクセス履歴情報送信要求部５６ｅにより前述した例においてはその中継装置２１に対してアクセス履歴情報の送信要求を送る。中継装置２１からアクセス履歴情報を受信すると、その内容から不正アクセスを行った端末装置５４が中継装置２１のポート２１ａ（ポート番号Ｐ１）側に存在することがわかる。逆に言うと、この時点で端末装置５４がポート番号Ｐ２側に存在しないことがわかる。次に、中継装置２１のポート２１ａにはＬＡＮ１５が接続されているので、ＬＡＮ１５に接続されている中継装置、本実施例においては中継装置２２、２３、２４に対してアクセス履歴情報の送信要求を送る。各中継装置２２、２３、２４からアクセス履歴情報を受信すると、上記と同様、不正アクセスを行った端末装置５４が各中継装置２２、２３、２４のどのポート側に存在しているかを管理装置５６が判定する。中継装置２２、２３においては、端末装置５４が中継装置２２、２３のポート２２ａ、２３ａ（ポート番号Ｐ１）側に存在することがわかる。一方、中継装置２４のアクセス履歴情報から端末装置５４が中継装置２４のポート２４ｂ（ポート番号Ｐ２）側に存在することがわかる。

【００４９】以上のようにして、管理装置５６は、アラーム情報とアクセス履歴情報とから不正アクセスを行った端末装置５４が中継装置２４のポート２４ｂに接続されたＬＡＮ１４上に存在することを特定することができる。なお、仮にＬＡＮ１４に中継装置２４以外の中継装置が接続され階層的なネットワーク構造になっていても上記方法を繰り返すことで不正アクセスを行った端末装置を特定することができる。この特定された内容を出力装置に表示させることで不正アクセスがあったことのみならず、中継装置から受信したアラーム情報により、どのＬＡＮに接続された端末装置からの不正アクセスであったかを特定しネットワーク管理者等に知らせることができる。

【００５０】なお、中継装置の接続位置の変更、伝送媒体の接続構成の変更や増設、端末装置の接続位置変更や端末装置の活性状態変更などが発生したことをなるべく早期に自動でアクセス履歴情報に反映するために、アクセス履歴情報の保持する内容に図６に示したようにタイマカウンタを追加する方法がある。例として端末装置５４から端末装置５１にフレームを送信する場合の中継装置２４の動作について説明するが、主要でない上記と同様の動作についての説明は省略する。なお、中継装置２４には、予めアクセス履歴情報をリフレッシュするリフレッシュタイム値（しきい値）を登録しておく。

【００５１】中継装置２４は、アクセス履歴情報部２１ｇに端末装置５４のアドレス（Ｘａｄｒ）と受信したポート番号Ｐ１を記憶する再に、端末装置５４のアドレス（Ｘ＿ａｄｒ）に対する記憶タイマカウンタ（Ｔｘ）を初期値ゼロとして登録する。以降、同じフレームを同じポートから受信したときも再度端末装置５４のアドレス（Ｘ＿ａｄｒ）を登録し記憶タイマカウンタ（Ｔｘ）を初期値ゼロとする。一方、タイマ割り込みにより一定時間間隔毎に図７の処理がコールされる。アクセス履歴情報部２１ｇの記憶タイマカウンタ（Ｔａ、Ｔｂ、Ｔｈ、Ｔｍ、Ｔｘ、Ｔｙ）とリフレッシュタイム値とを比較し、記憶タイマカウンタが大きければ、その記憶タイマカウンタに対応するアドレスを削除する。次に、記憶タイマカウンタに一定時間間隔にコールされる時間の相当分を加算してアクセス履歴情報の自動リフレッシュ処理を終了する。

【００５２】なお、本実施例は、不正アクセスの検出について説明したが、アラーム情報を管理装置に通知する条件の設定内容により他の検出にも応用することができる。

【００５３】また、本実施例は、管理装置により不正アクセスをした端末装置又は障害発生した端末装置を特定すること並びに端末装置が接続されている伝送媒体を特定することについて説明したが、一般の端末装置に管理装置５６に相当する機能を有するソフトウェアをインストールすることによっても実現することができる。

【００５４】

【発明の効果】以上のように、本発明によれば、中継装置は、許可／禁止情報並びにアラーム情報通知条件に基づいて不正アクセス等を検出すると、アラーム情報を管理装置に通知し、表示することができるので、ネットワーク管理者等が、不正アクセスがあったことを知ることが可能となる。

【００５５】また、アラーム通知条件登録手段を設けたことにより、上記アラーム情報を管理装置に通知する条件を任意に設定することが可能となる。

【００５６】また、送信要求をして得たアクセス履歴情報とアラーム情報とから不正アクセスをした端末装置を特定する手段を設けたことにより、不正アクセスがあったことを知ることができるのみならず、当該端末装置がどの伝送媒体に接続されているかを特定することが可能となる。

【００５７】また、管理装置は、上記管理装置における機能を付与することで一般の端末装置においても実現可能となる。

【図面の簡単な説明】

【図１】本発明に係るセキュリティ方式が実施されるネットワークシステムの構成図である。

【図２】本実施例における中継装置の構成を示した図である。

【図３】本実施例において、各中継装置が有しているアクセス履歴情報を示した図である。

【図４】本実施例における管理装置の構成を示した図である。

11　　12

【図５】本実施例における中継装置の処理を示したフローチャートである。

【図６】本実施例において、中継装置が有している記憶タイマカウンタを含むアクセス履歴情報を示した図である。

【図７】本実施例において、タイマ割り込みによりコールされる自動リフレッシュ処理を示したフローチャートである。

【図８】従来のローカルエリアネットワークシステムの構成図である。

【符号の説明】

１１、１２、１３、１４、１５　ＬＡＮ

２１、２２、２３、２４　中継装置

＊２１ａ、２１ｂ　ポート

２１ｃ　制御部

２１ｄ　中継制御テーブル

２１ｅ　アラーム情報通知部

２１ｆ　アラーム情報通知条件登録部

２１ｇ　アクセス履歴情報記憶部

５１、５２、５３、５４、５５　端末装置

５６　管理装置

５６ａ　入出力部

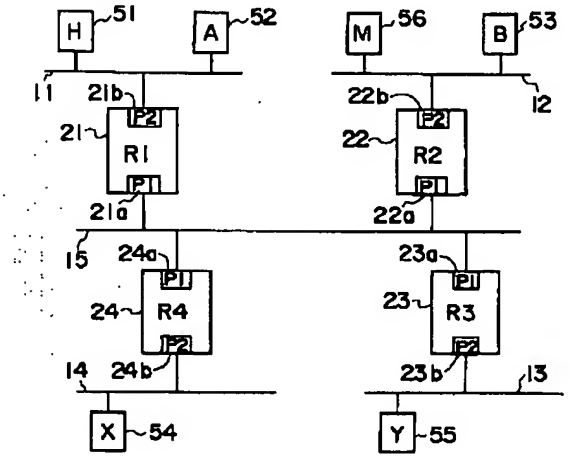
５６ｂ　制御部

５６ｃ　メモリ

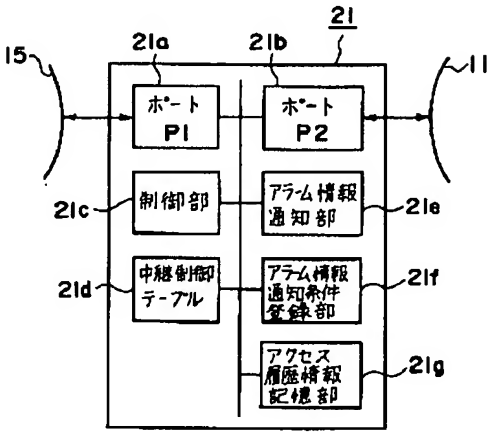
５６ｄ　アラーム情報表示部

５６ｅ　アクセス履歴情報送信要求部

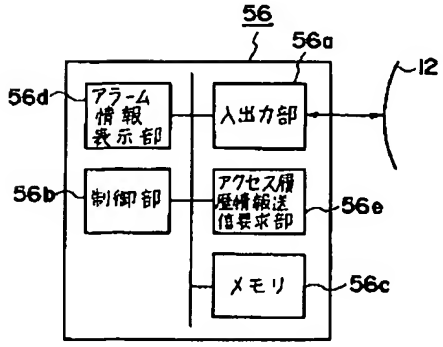
【図１】



【図２】



【図４】



【図６】

アドレス	ポート番号	記憶タイマカウンタ
A_adr	P1	Ta
B_adr	P1	Tb
H_adr	P1	Th
M_adr	P1	Tm
X_adr	P2	Tx
Y_adr	P1	Ty

【図３】

Ｒ１のアクセス履歴

アドレス	ポート番号
A_adr	P2
B_adr	P1
H_adr	P2
M_adr	P1
X_adr	P1
Y_adr	P1

Ｒ２のアクセス履歴

アドレス	ポート番号
A_adr	P1
B_adr	P2
H_adr	P1
M_adr	P2
X_adr	P1
Y_adr	P1

Ｒ３のアクセス履歴

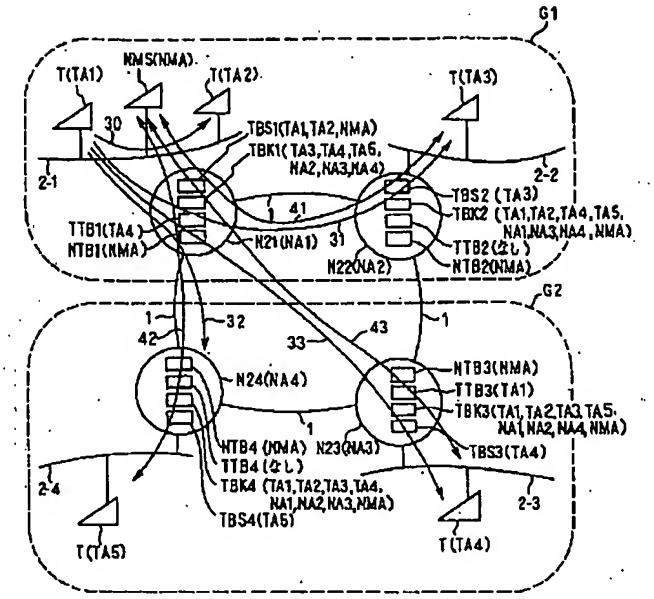
アドレス	ポート番号
A_adr	P1
B_adr	P1
H_adr	P1
M_adr	P1
X_adr	P1
Y_adr	P2

Ｒ４のアクセス履歴

アドレス	ポート番号
A_adr	P1
B_adr	P1
H_adr	P1
M_adr	P1
X_adr	P2
Y_adr	P1

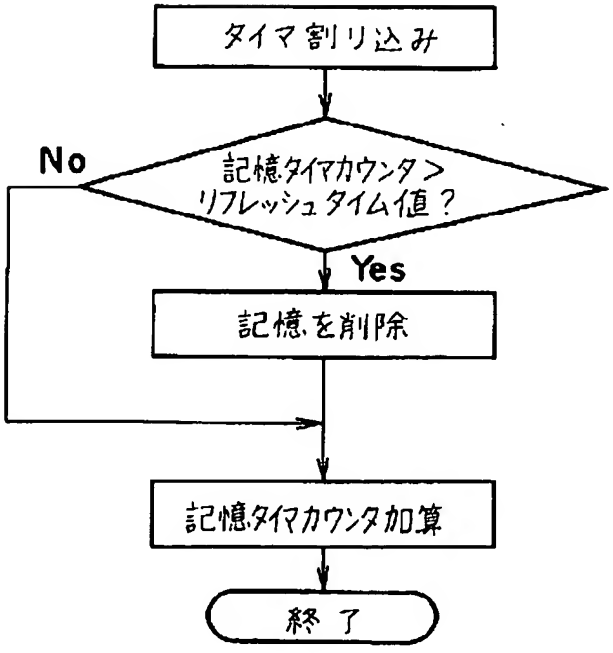
A_adr :端末装置Aのアドレス
B_adr :端末装置Bのアドレス
H_adr :端末装置Hのアドレス
M_adr :端末装置Mのアドレス
X_adr :端末装置Xのアドレス
Y_adr :端末装置Yのアドレス

【図８】

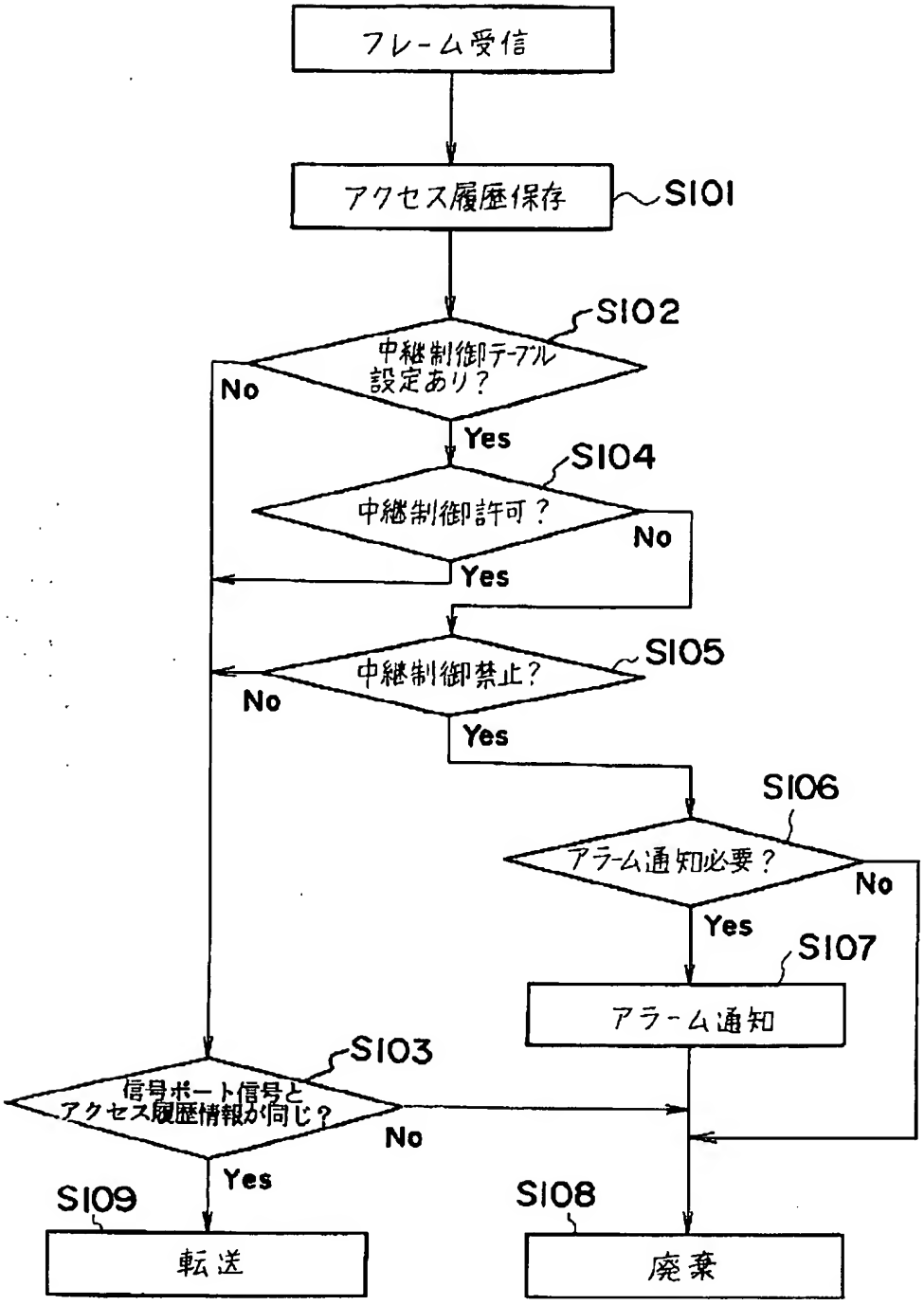


1 : 幹線ローカルエリアネットワーク
2-1～2-4 : 支線ローカルエリアネットワーク
N21～N24 : ノード装置
NA1～NA4 : ノード装置のアドレス
T : 端末装置
TA1～TA5 : 端末アドレス
TBS1～TBS4 : 支線側フィルタリングテーブル
TBK1～TBK4 : 幹線側フィルタリングテーブル
TTB1～TTB4 : 特権端末テーブル
NTB1～NTB4 : NMSアドレステーブル
G1, G2 : グループ番号
NMS : ネットワーク管理局
NMA : ネットワーク管理局のアドレス
30～33 : 端末装置間の通信を示す矢印
40～43 : NMSと端末装置間の双方向の通信を示す矢印

【図７】



【図5】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI	技術表示箇所
G06F	13/00	351	Z 7368－5B		
	15/00	330	A 7459－5L		
H04L	12/40				